REMARKS

Amendments to the Claims

Claim 10 is amended to change "whereby" to "comprising:" in line 5 to more properly recite the inventive subject matter in terms reflecting appropriate U.S. practice. The scope and meaning of the claim is unchanged by the amendment.

Claim 13 is amended to correct an obvious mistake resulting from the original claim referring back to claim 9 instead of claim 10. The claim has been amended to properly refer back to claim 10.

Claim Rejections – 35 USC §102

The rejection of claims 1-6 and 8-14 under 35 USC §102(e) as being anticipated by Russo (U.S. 2003/0101348 A1) is respectfully traversed. As a starting point, the scope and meaning of the claims are reviewed from the perspective of a person skilled in the art based on the written description and drawings of the application.

Claim 1 recites a method for effecting a secure electronic transaction on a terminal using a portable data carrier that is capable of performing different quality user authentication methods. It is important to note that the terminal is a separate device from the portable data carrier and that the portable data carrier is capable of performing a user authentication using one of the different user authentication methods varying between an inherently relatively lower quality and an inherently relatively higher quality of user authentication, and further wherein the data carrier creates authentication quality information about the user authentication method and attaches the authentication quality information to the result of the security establishing operation carried out by the portable data carrier.

An important point to note is that the portable data carrier performs the security establishing operation after the initial user authentication procedure performed by the portable data carrier (claim 1, line 5).

Thus, the user authentication carried out by the portable data carrier is a separate and distinct operation from the authentication quality information generated by the portable data carrier during a secure electronic transaction.

The original description explains the process in more conventional language, particularly in the description spanning pages 3 and 4 of the specification. As explained in the paragraphs spanning pages 3 and 4, the terminal has an interface (19) for communication with a portable data carrier (20). The data carrier may be of the contact or non-contact type.

The terminal includes various sensor devices (15) for sensing biometric information. The portable data carrier (20) may be a chip card that communicates with the terminal via the interface (19). Accordingly, communication between the terminal and chip card is enabled (specification, page 4, second paragraph).

The portable data carrier itself is set up to perform at least one but expediently a plurality of different quality user authentication methods, preferably at least two different authentication methods having a different order of security. For example, it may support at least one knowledge-based authentication method (a PIN check), and at least one biometric method. Obviously, the biometric method inherently constitutes a higher quality method of authentication as compared with the knowledge-based authentication method (*id.*, page 5, first paragraph). The smart card has a storage means (26) that stores at least one secret to be presented to the user, for example a reference PIN assigned to the user and at least one biometric reference data record assigned to the user.

Of significant importance is the fact that, after the signature application has been started, the user presents a suitable portable data carrier (20) to the terminal (40 – step 104) following which the terminal recognizes the presence of the chip card and performs a mutual authentication therewith (*id.*, step 106) wherein the chip card first proves its authenticity to the terminal and then the terminal to the chip card (*id.*, page 6, lines 1-3).

If authentication is successful, the terminal and chip card negotiate dynamic session keys to permit further communication to be conducted securely in the so-called secure messaging mode (*id.*, step 108). Then, authentication of the user vis-à-vis the chip card 20 is effected. First the terminal 14 checks how authentication is to be effected (e.g., knowledge-based or biometrically). If the authentication is by the PIN method, the user enters the PIN via the input means (18) to the terminal (14) that passes it on directly or in modified form via the interface (19, 22) to the chip card 20 (*id.*, page 6, penultimate paragraph). The total communication between terminal 14 and chip card 20 is expediently effected in the secure messaging mode.

The chip card then checks the transmitted PIN and confirms correctness of same to the terminal if there is no error, or terminates the procedure if the PIN was checked as false (*id.*, step 116).

If the no-error case is given, the terminal causes the chip card by corresponding instructions to perform the security establishing operation, i.e. the digital signature, and transmits the electronic document to be signed to the chip card.

The chip card signs the supplied electronic document with the secret key stored in the storage means 22 (step 120) and sends the electronic signature back to the terminal (step 122) which uses it to continue the initiated electronic transaction (*id.*, page 7, second paragraph).

If the authentication of the user is to be biometric, the terminal (14) initiates authentication against presentation of a biometric feature and makes a corresponding report to the chip card 20 (step 130).

After the detected biometric feature is analyzed at the terminal, involving extraction of certain key features, the extracted features are then transmitted by the terminal to the portable data carrier (*id.*, page 7, penultimate paragraph – step 138).

Significantly, when the data carrier receives the information from the terminal, it performs a separate verification of the transmitted extracted features (step 140). The circuit of the data carrier compares the received extracted features with the reference features stored in the storage means of the data card and checks whether a sufficient match is present. If the match is correct, the data carrier confirms same to the terminal that verification of the transmitted biometric feature has been successfully carried out. Portable carrier then switches itself ready to executed the intended security establishing operation (*id.*, paragraph spanning pages 7 and 8).

Accordingly, it will be evident that, in accordance with the present invention as claimed in claim 1, it is the data carrier that performs a security establishing operation within the electronic transaction using a hardware token in the form of the portable data carrier. Initial authentication step is carried out separately from the later security establishing operation whereby the terminal communicates information regarding the authentication process to the portable data carrier that then attaches authentication quality information to the result of the security establishing operation.

Claim 2 further modifies the method recited in claim 1 by reciting that the security establishing operation performed by the portable data carrier comprises creating a digital signature.

Claims 3, 4 and 5, respectively recite that the authentication of the user is performed by presentation of a biometric feature, a physiological or behaviour-based feature or proof of knowledge of a secret.

In accordance with claim 6, at least two different authentication methods of different quality are offered for authentication of the user.

Claim 7 specifically recites that the particular authentication methods not used by the portable data carrier are disabled (figure 2, step 112; figure 3, step 132).

Claim 8 further modifies claim 6 by reciting that no quality information is produced for an authentication method.

Claim 9 further modifies claim 1 by reciting that the user is asked to select an authentication method.

Claim 10 is an independent claim reciting the portable data carrier wherein the data carrier is arranged to perform a user authentication using one of the implemented user authentication methods and further is arranged to confirm the authentication to a terminal, wherein the data carrier is arranged to create quality information about said user authentication method used and to attach such quality information to the result of the security establishing operation.

Claims 11 and 12 further refine the description of the portable data carrier according to claim 10, wherein the portable data carrier is set up to create a digital signature (claim 11) or the data carrier supports at least two qualitatively different authentication methods (claim 12).

Claim 13 recites a terminal for use in connection with the portable data carrier according to claim 10 wherein the terminal includes a device arranged to cause a user to select at least one of two possible different quality authentication methods.

Claim 14 recites a system for effecting a secure electronic transaction within which the quality of authentication of a user of the system is ascertained, comprising the portable data carrier according to claim 10 and the terminal according to claim 13.

The primary reference relied on by the examiner in rejecting claims 1-6 and 8-14, namely Russo, discloses a method and system that uses software tokens to indicate risks in connection with the authentication of a client using the system. That is, the secret (e.g. a password or private key) of a user that is used to authenticate the user against the system is associated with additional data (the so-called "software" confidence token) which data includes information ("trust metric") about the risk that the secret is compromised. (Russo, [0039], [0043], [0044], [0047]). The trust metric may also contain information about the strength of an authentication method that is used for user authentication (*id.*, [0007], [0008], [0050]).

In addition to the aforesaid trust metric, the software token of Russo comprises transaction information (*id.*, [0046]) which defines the transaction that is requested by the user.

Both transaction information and trust metric are included in an "envelope" which is then "sealed" by means of a secret containing a digital signature in order to complete the confidence token. In general, the digital signature is created with a secret key of the user (*id.*, [0053]) which key is part of a PKI infrastructure (*id.*, [0038]).

When the server receives the confidence token, it first verifies the signature, e.g. with the respective public key of the user. If the verification is successful, the server finally determines the confidence of the transaction according to the trust metric extracted from the confidence token and completes the transaction if the level of confidence indicated by the trust metric is high enough (*id.*, [0058-60]).

Accordingly, it is clear that Russo is incapable of anticipating at least claims 1 and 10, as it fails to show, teach or suggest a portable data carrier that performs a security establishing operation within the electronic translation after the portable data carrier performs a user authentication using one of different user authentication methods. There is no teaching in Russo of using a portable data carrier in the manner recited in claims 1 and 10, particularly wherein the data carrier attaches authentication quality information to the result of a security establishing operation following an initial user authentication procedure initiated between the portable data carrier and the terminal.

While Russo mentions the use of smart cards in the written description of the published application, the smart cards are used to support a specific authentication method during user authentication (using something you have) but none of the data carriers is arranged to perform different quality user authentication methods and to perform user authentication using one of the different user authentication methods. None of the smart cards of Russo is arranged to perform a security establishing operation within the electronic transaction. Russo neither discloses nor suggests a data carrier to create an authentication quality information and to attach that authentication quality information to the result of the security establishing operation. Rather, Russo requires that the trust metric be determined by the requester in the manner explained in paragraphs 0048-0051.

Russo fails to disclose any security establishing operation that is separate from a step of authenticating the user. For example, the step of sealing the envelope (*id.*, [0024, 0053]) in order to complete the confidence token, such step involving a digital signature based on a

secret key of the user, is basically used to authenticate the transaction, i.e. to authenticate the user requesting the transaction. The server of Russo verifies this signature based on the public key of the user (*id.*, [0059]) wherein the server authenticates the user by verifying the signature. Thus, the digital transaction that is requested by the requester according to Russo may not even require any other security establishing operation.

As a result, the trust metric of Russo, which may be interpreted to represent the authentication quality information of the present invention, cannot be attached to the result of the security establishing operation, since there is no security establishing operation disclosed within Russo and hence it cannot be a result of such an operation. According to Russo, the trust metric is attached to the transaction information (*id.*, [0046]) which merely defines a transaction that is requested to be performed by the server.

In short, in accordance with Russo, a digital transaction is requested (not yet performed) at a server together with a quality information concerning the authentication of the user. Based on this quality information, the server decides whether or not to execute or complete the requested transaction. Contrasted with such a procedure, in accordance with the present invention, it is the data carrier after successful authentication of the user, that actually performs the security establishing operation in connection with the digital transaction and attaches an authentication quality information to the result of the security establishing operation. As a result of the invention, third parties may then evaluate the result of the transaction according to the authentication quality information.

Due to the clear absence in Russo of any teaching of features recited in independent claims 1 and 10, withdrawal of the rejection of these claims under 35 USC§102(e) is appropriate and the same is respectfully requested. Claims 2-6, 8, 9, 11-14 are likewise patentable at least on the basis of the patentability of the claims from which they depend or which they incorporate.

Claim Rejections – 35 USC §103

The rejection of claim 7 as being unpatentable over Russo in view of Miyashita is respectfully traversed. For reasons given above, it is clear that Russo is not appropriate as a basic reference that may be modified by Miyashita in the manner suggested by the examiner to result in a teaching of obviousness of claim 7. Even if Miyashita is somehow incorporated within the teachings of Russo, the combination of teachings still fails to establish *prima facie*

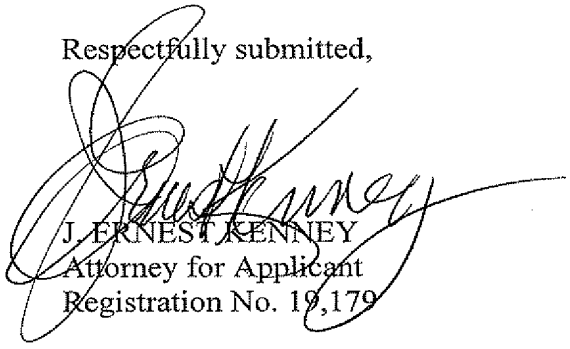
obviousness of claim 7, which requires all the features of claim 1, which features are not shown or taught in Russo.

Accordingly, withdrawal of the rejection of claim 7 under 35 USC §103(a) is appropriate and the same is respectfully requested.

Applicant submits that this application is in condition for allowance and its passage to issue is respectfully requested.

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, VA 22314-1176
Phone: (703) 683-0500
Facsimile: (703) 683-1080
Date: May 27, 2010

Respectfully submitted,



J. ERNEST KENNEY
Attorney for Applicant
Registration No. 19,179